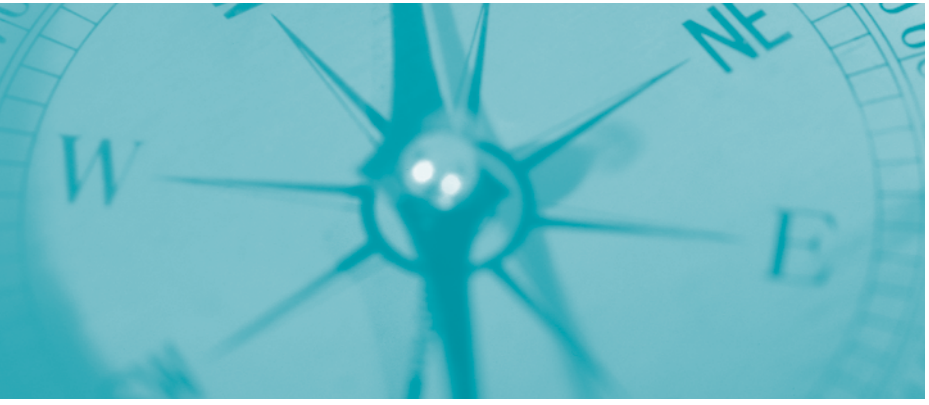
Managing the Intelligence Function



7

CHAPTER SEVEN

Managing the Intelligence Function

Most American law enforcement agencies will not have a formal intelligence unit, but will still have an intelligence function to manage. With the growing symbiosis among federal and state, local, and tribal law enforcement (SLTLE), adoption of the National Criminal Intelligence Sharing Plan and the growth of networked intelligence information systems, along with the responsibility to keep the homeland secure, virtually every law enforcement agency in the country needs to develop some type of intelligence capacity. That capacity may be a full-scale unit or one person who serves part time as an agency's point of contact to receive and disseminate critical information. In some form, an intelligence capacity has become a de facto requirement for U.S. law enforcement agencies. As a result, new intelligence processes for SLTLE provides challenges such as the following to the executive:

- Reengineering some of the organization's structure and processes
- Developing a shared vision of the terrorist or criminal threat among all law enforcement agencies in the region and at the federal level.
- Participating in intelligence processes and following through with threat information
- Committing resources, time, and energy to the intelligence function
- Developing a proactive spirit and creative thought to identify "what we don't know" about terrorism and international organized crime
- Developing a culture within the law enforcement agency that is able to think globally and act locally
- Providing vigilance, patience, and entrepreneurial leadership.

To operationalize these components into a functional intelligence mechanism, SLTLE agencies of all sizes need, at a minimum, fundamental operational components. These include the following:

- A person designated as the intelligence point of contact to whom external agencies may direct inquiries, warnings, and advisories and from whom information and questions may be sent. This person must have sufficient training to understand the language, processes, and regulations incumbent on the law enforcement intelligence community.
- A secure electronic communications system for sending and receiving information that is Law Enforcement Sensitive (LES) and For Official Use Only (FOUO). Several systems are available, including Law Enforcement Online (LEO), RISS.net, Anti-Terrorism Information Exchange (ATIX), National Law Enforcement Telecommunications System (NLETS), and Joint Regional Information Exchange System (JRIES) – some of which are available at no charge to the user. With the growth of the XML standard,[123] access to these systems will be essential for the most accurate information sharing.
- Established policies for information collection, reporting, and dissemination. If an agency of any size is going to maintain intelligence records, the agency must have policies in place to control that data or risk exposure to liability. In many cases, adoption of the Law Enforcement Intelligence Unit (LEIU) File Guidelines (see Appendix B) will serve the purpose.

123 For information on the Global Justice Information Standard, see http://it.ojp.gov/topic.jsp?topic_id=43.

- Establishing the ability to determine the kinds of information/intelligence that is needed to effectively prevent terrorism and disrupt criminal enterprises. This is a more difficult challenge and requires a greater labor investment. Understanding the threats and targets within a community and developing responses to neutralize those threats is essential. As observed by FBI Executive Assistant Director of Intelligence Maureen Baginski, "The absence of evidence is not the absence of a threat."[124] It is essential that American law enforcement discover the evidence that may be in its backyard.

Beyond these factors, a number of management factors may be considered when developing an intelligence capacity. This chapter provides a perspective on issues from which the reader may choose those applicable elements that apply to one's respective law enforcement organization.

Establishing an Organizational Framework

124 Baginski, Maureen, EAD-I, Federal Bureau of Investigation. Remarks in an address to the Major City Chiefs Intelligence Commanders Conference. Washington, DC. May 2004.

Just as any other function in a law enforcement agency, organizational attention must be given to the administrative structure of the law enforcement intelligence (LEI) unit. Administrators and managers must examine the following:

- The ***need*** for the LEI unit
- How it functions every day
- Issues of ***resource*** acquisition, deployment, and management
- ***Future agency needs*** for the intelligence function.

Properly organized and staffed, the intelligence function serves as an internal consultant to management for resource deployment. It should be designed as an integrated and organic element of the law enforcement organization, not a distinct function. Intelligence defines the scope and dimensions of complex criminality – including terrorism – facing the jurisdiction and provides alternatives for policy responses to those problems. Importantly, it also serves as a focal point for information sharing and dissemination to maximize community safety. Some law enforcement agencies have been reluctant to fully develop an intelligence unit – including both tactical and strategic activities – for several reasons.

Perhaps at the top of the list is the past abuses and subsequent lawsuits from poorly organized and managed intelligence activities. In many cases, law enforcement executives eliminated the intelligence unit to reduce liability and to minimize criticism from persons in the community who did not understand the intelligence role and/or generally opposed law enforcement intelligence for philosophical reasons. Similarly, the need and value of an LEI unit has not been fully recognized by managers who often do not understand that the intelligence function can be an important resource for agency planning and operations. For example, intelligence analysts are frequently assigned clerical tasks instead of proactive analysis, largely because the manager does not recognize the value of intelligence analysis as a management resource.

Properly ORGANIZED and STAFFED, the intelligence function serves as an internal consultant to management for RESOURCE DEPLOYMENT.

As a consequence of several factors, the Zeitgeist – or "spirit of the times" – is now present for American law enforcement to embrace law enforcement intelligence of the 21st century. Many SLTLE agencies have established a legacy of proactive law enforcement through the use of community policing and its activities of problem solving, CompStat, crime analysis, effective internal and external communications, multidisciplinary responses to crime, and a "bottom-up" approach for operational direction. Moreover, since 9/11, there has been a greater development of resources and training to make intelligence activities more easily adapted and functional. Finally, the law enforcement intelligence function has become professionalized through greater involvement of academic institutions, federal initiatives, and long-standing activities by groups such as the International Association of Law Enforcement Intelligence Analysts (IALEIA) and the Law Enforcement Intelligence Unit (LEIU).[125]

125 For more information on these organizations see their respective web pages at http://www.ialeia.org and http://www.leiu-homepage.org.

"Chartering" an Intelligence Unit

One of the first steps in creating an intelligence unit is to "charter" the function. This includes the following:

- Determining its organizational priority and placement
- Resource allocation
- Defining its mission and goals
- Establishing the unit's authority and responsibility,

A number of publications describe these processes.[126] The current discussion will identify specific points related to the intelligence function. The creation of an intelligence unit should be based on a needs assessment.[127] This includes identifying current intelligence-related competencies of the law enforcement agency and desired competencies. One of the main outcomes of an effective needs assessment is identifying how an intelligence unit can influence the drive toward greater efficiency and responsiveness. Importantly, the needs assessment will also define personnel and resource needs.

Resource allocation is always a difficult process because it typically involves diminishing one function to develop another. In most cases, the creation of a new unit will not come with a new appropriation of funding to fully staff and operationalize it; therefore, part of the resource allocation process is to determine where the intelligence function fits in the organizational priorities of the law enforcement agency.

The mission is the role that the unit fulfills in support of the agency's overall mission. It specifies in general language what the unit is intended to accomplish and establishes the direction and responsibility for the LEI unit for which all other administrative actions and activities are designed to fulfill. Figure 7-1 presents a sample mission statement for a law enforcement agency's intelligence unit.

A goal is the end to which all activity in the unit is directed. It is broad based, yet functionally oriented. Importantly, the goal must be mission-related, that is, accomplishing goals supports the broader mission of the

126 Most police management textbooks describe these processes in detail. Perhaps of particular value are publications available from the International City Management Association http://bookstore.icma.org. See also the on-line performance management database of the Royal Canadian Mounted Police at http://www.rcmp-learning.org/fr-welc.htm.

127 A good illustration of a law enforcement needs assessment and how it can be performed, which includes multiple applications is: Healy, J.J., Superintendent, International Training and Peacekeeping Branch, Royal Canadian Mounted Police. http://www.rcmp-learning.org/docs/ecdd1134.htm.

law enforcement agency. Moreover, the goals will give the unit direction in support of the mission. Since the mission of an LEI unit will be comprehensive and incorporate diverse functions, several goals will be stipulated. The purpose of goals is to not only provide operational direction but to also serve as performance standards.[128] The environment of the community will change over time as will crime patterns and problems; therefore, the law enforcement agency should review goal statements annually and change or revise them to reflect current issues and trends. (Figure 7-1 also includes an illustration of intelligence goals for a law enforcement agency.)

Authority is the right to act or command others to act toward the attainment of organizational goals. Operational authority includes decisions that must be made concerning the degree and type of activities the LEI unit may perform without seeking administrative authorization, financial flexibility of the unit to fulfill its objectives, and the degree of direction or precedence the LEI unit can exercise over other departmental units. Each of these factors has significant organizational implications and must be developed conceptually and stipulated by policy.

128 Performance standards are often characterized as effectiveness and efficiency, wherein effectiveness is "Doing the right job." and efficiency is "Doing the job right."

Figure 7-1: Sample Mission Statement and Goals of an LEI Unit

Sample Intelligence Mission Statement

The mission of the Intelligence Unit of the Hypothetical Police Department is to collect, evaluate, analyze, and disseminate intelligence data regarding criminal activity in this city/county and any criminal activity in other jurisdictions that may adversely effect on this city/county. This includes providing processes for collating and analyzing information collected by operational units of the law enforcement agency. The Intelligence Unit will furnish the Chief of Police with the necessary information so that Operations Units charged with the arrest responsibility can take the necessary enforcement action.

Sample Intelligence Goals

1. The Intelligence Unit shall supply the Chief of Police with accurate and current strategic intelligence data so that the Chief will be kept informed of changing criminal activity in the jurisdiction.

Figure 7-1: Sample Mission Statement and Goals of an LEI Unit (Cont.)

2. The Intelligence Unit shall provide a descriptive analysis of organized crime systems operating within the jurisdiction to provide operational units with the necessary data to identify organized crime groups and individuals working as criminal enterprises.

3. The Intelligence Unit will concentrate its expertise on the following crimes…

   a. Islamic extremists in support of terrorism – activities, participants, funding, and logistical support, all of which are of a criminal nature.

   b. Domestic extremists in support of criminal acts – activities, participants, funding, and logistical support, all of which are of a criminal nature.

   c. Labor/strike activity – monitor and gather strategic intelligence to be supplied to the Operations Bureau with regard to this activity.

   d. Organized crime – identify crimes and participants, including new and emerging criminal enterprises.

   e. Major Narcotics Traffickers – provide tactical intelligence and information analysis to the Operations Bureau on persons identified as being involved in narcotics trafficking enterprises.

The Intelligence Unit recognizes the delicate balance between the individual rights of citizens and the legitimate needs of law enforcement. In light of this recognition, the unit will perform all of its intelligence activities in a manner that is consistent with and upholds those rights.

129 http://it.ojp.gov/process_links.jsp?link_id=3774

Responsibility reflects how the authority of a unit or individual is used for determining if goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority. The unit and its members must be held accountable for its charge and administrative mechanisms must be set in place to assess the degree to which the unit is meeting its responsibilities.

IACP Model Policy on Criminal Intelligence.

The International Association of Chiefs of Police (IACP) has taken a proactive role in all aspects of developing a contemporary intelligence capacity in America's law enforcement agencies. The IACP Model Policy[129]

on Criminal Intelligence provides a policy statement and procedures that are of particular benefit to a small agency. As in the case of all models, the language of the IACP policy needs to be adjusted to meet the needs of different jurisdictions. Nonetheless, it provides a sound foundation for starting the process.

Adhering to 28 CFR Part 23

Throughout this guide, reference is made to a federal regulation entitled Criminal Intelligence Systems Operating Policies, cited as 28 CFR Part 23. As is becoming apparent, it is essential that SLTLE intelligence records system adhere to the provisions of this regulation if the system is a multi-jurisdictional and supported with federal funding. The best way to demonstrate and ensure adherence is for the law enforcement agency to develop specific policies and procedures to cover segments of the regulation, including the following:

- Security
- Accessing the system to make inquiries
- Defining standards for identifying and classifying "Non-Criminal Identifying Information"
- Entering data in the criminal intelligence system
- Reviewing data quality and propriety
- Purging
- Disseminating intelligence.

Even if 28 CFR Part 23 guidelines do not apply to a specific law enforcement agency, use of the guideline and these policies is good practice for the agency to follow.

Auditing the Intelligence Function

Perhaps one of the best ways to understand management of the intelligence unit is to examine the variables used in the audit process. Appendix C is an audit questionnaire created by the author that includes 180 variables to assess in an intelligence audit. The necessity for an audit is essential for both operational reasons and risk management. By

reviewing the questionnaire, which has been used by the author to assess compliance with a U.S. District Court settlement in one city's intelligence unit, it will become clear that there are myriad factors that are incumbent on ensuring organizational control of the intelligence function.

In addition, the Global Intelligence Working Group and the LEIU are preparing intelligence unit audit guidelines. At the time of this writing, the guidelines were not completed; however, they will likely appear on the Global Intelligence Working Group website when they available and ready for distribution.[130]

Establishing and Managing Partnerships

The nature of the intelligence function requires that a law enforcement agency enter into partnerships. Critical information is shared through collaboration, typically with other law enforcement agencies, but often with other organizations ranging from private security to non-law enforcement government agencies, such as public health or emergency services. These various relationships have different dynamics related to needs, responsibilities, and limitations on access to information. As such, the parameters of each formal partnership should be articulated in a formal partnership agreement.

130 http://it.ojp.gov/topic.jsp?topic_id=56

Critical information is shared through collaboration, typically with other law enforcement agencies, but often with

Broadly speaking, two types of partnerships are related to the intelligence function. These are the following:

- ***Users:*** Organizations with which information and/or intelligence products are shared. Users are consumers.
- ***Participants:*** Organizations that provide resources and actively contribute to the intelligence activity, such as a regional intelligence center. Participants have a shared responsibility for operations.

A formal agreement is simply sound management because it articulates mutually agreed-on operational provisions related to resource management; clear identification of responsibilities and accountability; adherence to legal standards; and conditions associated with liability. Certainly these agreements apply to a wide range of law enforcement activities or services; however, the current discussion is limited to the intelligence function. While the language varies between states, as a general rule there are three forms of written partnerships:

- ***Memorandum of Agreement (MOA):*** Users/consumers of an intelligence unit or system, including a records system, that use the system on an ongoing basis would typically sign the MOA. Essentially, the MOA acknowledges that the user will abide by the "rules" established for the system or activity, aid in cost recovery, and adhere to legal and accountability standards. Obviously, the character of the activity will dictate more detail. As an example, if one agency's intelligence records system can be accessed by another agency, the user may have to agree to pay a monthly fee, adhere to 28 CFR Part 23, and agree to the Third Agency Rule. Failure to meet these standards would result in ending access to the system.
- ***Mutual Aid Pact (MAP):*** The MAP is an agreement that is in place to deal with special circumstances, rather than an ongoing service, and establishes the agreed-on conditions when one agency would provide assistance to another. Oftentimes assistance is reciprocal, except for real costs that may be incurred in extended activities. As an intelligence-related example, two law enforcement agencies may agree to aid each other when conducting a surveillance.
- ***Memorandum of Understanding (MOU):*** The MOU is more detailed and involves a partnership in an activity. Essentially a contract, the MOU would specify all obligations and responsibilities and typically share liabilities in the endeavor. For example, if multiple agencies agree to develop a regional intelligence center, the MOU may be a fairly detailed document outlining all aspects of governance, management, structure, funding, accountability, and operations of the center.

A key element to understand is that, regardless of the nature of the agreement, its content and detail is to ensure that all parties understand

their obligations. Figure 7-2 identifies some of the provisions that may be included in a partnership agreement. While not all of these provisions will be required of every agreement, it is important to have a formal document that clearly defines expectations and responsibilities.

Figure 7-2: Sample Provisions for a Partnership Agreement

- Activities
- Civil liability/indemnification
- Dispute resolution
- Funding
- Governance
- Information – access and use
- Information – adherence to 28 CFR Part 23
- Information – dissemination to "Third Agency"
- Information – entry into a system
- Information – ownership
- Location
- Mission, purpose, goals
- Operating procedures
- Payments and costs
- Personnel assignment
- Personnel evaluation
- Personnel removal
- Physical plant considerations
- Property - purchase and maintenance
- Reports to be prepared
- Security clearances of staff
- Security of information
- Security of the facility
- Time limit/term of the agreement

Sources for Intelligence Management and Resource Trends

Effective management of an intelligence unit requires that the manager be constantly informed of emerging issues, technologies, and trends. This is a difficult process; however, one of the more effective methods is to monitor online newsletters of reliable organizations. Topics can range from actions and activities of extremists groups to new products and new policy and legislation. As an illustration (not an endorsement), some of the more substantive news letters include (in alphabetical order) the following:

- Anti-Defamation League http://www.adl.org/learn/default.htm – there are two newsletters – the ***Law Enforcement Newsletter*** and the ***Breaking News***
- Center for Digital Government (three newsletters; one specifically on homeland security) http://www.centerdigitalgov.com/center/enewsletters.phtml
- ***Computer and Information Security*** http://www.securitypipeline.com (newsletter subscription in lower left portion of homepage)

- ***Federation of American Scientists Secrecy News***: http://www.fas.org/sgp/news/secrecy/
- ***Foundation for Defense of Democracies Weekly Update***: http://www.defenddemocracy.org/ (subscription is toward the bottom of the left side of the page – enter your email address.)
- ***Government Computer News*** http://www.gcn.com/profile/
- ***Government Computing*** http://www.kablenet.com/kd.nsf/EmailListFormNew?OpenForm
- ***Government Technology*** http://www.govtech.net/magazine/subscriptions/mailings.php?op=getaddy
- ***Homeland Security Institute Newsletter***: http://www.homelandsecurity.org/newsletterSignup.asp
- ***Homeland Security Update*** (DFI International) http://www.dfi-intl.com/shared/updates/subscribe.cfm?nav=2&homeland=1
- ***Homeland Security Week*** http://www.govexec.com/email/
- Information Warfare and Cyberterrorism http://www.iwar.org.uk/mailman/listinfo/infocon/
- Israeli Defense Force Intelligence and Terrorism Research Center http://www.intelligence.org.il/eng/main.htm#
- National White Collar Crime Center http://www.nw3c.org/contact.cfm (One can sign up for both the electronic and print versions of the newsletter on this page.)
- PoliceOne.com (***Law Enforcement News***) http://www.policeone.com/policenews/ (newsletter subscription on right side of home page)
- Saudi-U.S. Relations Information Service (quite a bit of information on terrorism http://www.saudi-us-relations.org/newsletter/saudi-us-newsletter.html (subscription box on left side under menu items)
- Southern Poverty Law Center http://www.splcenter.org/center/subscribe.jsp
- ***Terrorism Central Newsletter*** http://www.terrorismcentral.com/Newsletters/CurrentNewsletter.html
- Terrorism Research Center http://www.terrorism.org/mailman/listinfo (three newsletters)

- U.S. Department of Homeland Security, Office of Domestic Preparedness http://puborder.ncjrs.org/listservs/subscribe_odp.asp
- U.S. Department of Justice, Justice Technology Network http://www.nlectc.org/justnetnews/nlectc_subscribe.asp
- U.S. Department of State, Overseas Security Advisory Center (OSAC) http://www.ds-osac.org/newsletters.cfm (several newsletters available by subscription)

As is the case with any information, a newsletter will reflect the agenda of its sponsor. Keeping this in mind, valuable information can be gained for an intelligence manager to remain current on the issues for which one is responsible.

CONCLUSION

As a rule, the application of management principles may be applied generally regardless of the unit or assignment within a law enforcement agency. It is just as true that some substantive knowledge of the unit or function must also be developed. Criminal investigation commanders need to understand caseload differentials for crimes, patrol commanders must know minimum staffing requirements to handle calls for service, and traffic commanders must understand traffic analysis and its application to selective enforcement. It is no different with the intelligence commander. This chapter identified critical substantive elements of the intelligence function that will aid the law enforcement manager to manage this activity more effectively.